Alexander Joel

In the Aug. 14 issue of the *New York Times*, reporter Charles Savage describes whistleblower actions taken by former State Department employee John Napier Tye. Tye, who was the section chief for Internet freedom in the State Department's Bureau of Democracy, Human Rights, and Labor before stepping down in April, questioned whether the rules governing certain overseas intelligence surveillance activities adequately protect information that intelligence agencies "incidentally collect" about Americans while targeting the communications of foreign nationals overseas. In a *Washington Post* op-ed on July 18, Tye pointed out that such intelligence collection may be regulated not by the Foreign Intelligence Surveillance Act (FISA), but by Executive Order 12333. That order, updated in 2008 by President George W. Bush, helps govern the activities of the intelligence community.

Under EO 12333, intelligence agencies may collect, retain, and disseminate information about Americans "only in accordance with procedures … approved by the Attorney General … after consultation with the Director [of National Intelligence]." Tye noted that he is not familiar with the details of these procedures, but nonetheless said that Americans should be troubled by "the collection and storage of their communications" under the executive order.

As the civil liberties protection officer for the director of national intelligence (DNI), I work with intelligence agencies on these procedures, and would like to describe how they safeguard privacy and civil liberties.

But first I want to commend Tye for raising his concerns through the processes established for that purpose. Using those processes, he has been able to review his concerns with intelligence oversight bodies as well as with the public, all while continuing to protect classified information.

At the outset, remember that FISA, with very limited exceptions, requires the government to seek an individualized court order before it can intentionally target a United States person anywhere in the world to collect the content of his or her communications. The FISA court must be satisfied, based on a probable cause standard, that the United States person target is an agent of a foreign power, or, as appropriate, an officer or employee of a foreign power.

But even when the government targets foreign nationals overseas in response to valid foreign intelligence requirements, it will inevitably collect some communications about Americans. As the Privacy and Civil Liberties Oversight Board noted in its examination of Section 702 of FISA, "[t]he collection of communications to and from a target inevitably returns communications in which non-targets are on the other end, some of whom will be U.S. persons." Indeed, when Congress first enacted FISA in 1978, it required the government to follow what are called "minimization procedures" to "provide vital safeguards because they regulate the acquisition, retention, and dissemination of information about U.S. persons, including persons who are not authorized targets of surveillance."

Similarly, EO 12333 requires procedures to minimize how an agency collects, retains or disseminates U.S. person information. These procedures must be approved by the attorney general, providing an important additional check. The National Security Agency's procedures are reflected in documents such as United States Signals Intelligence Directive SP0018 (USSID 18), issued in 1993 and updated in 2011. These procedures generally provide that communications may not be retained for more than five years. In addition, NSA personnel may not use U.S. person "selection terms" (such as names, phone numbers or email addresses) to retrieve communications from its collection under EO 12333 without a finding by the attorney general that the U.S. person is an agent of a foreign power (or in other similarly narrow circumstances). And even if the NSA determines that information about an American constitutes foreign intelligence, it generally uses a generic label like "U.S. Person 1" in intelligence reporting to safeguard the person's identity. The underlying identity may be provided only in a very limited set of circumstances, such as if it's necessary to understand the particular foreign intelligence being conveyed.

Oversight is extensive and multi-layered. Executive branch oversight is provided internally at the NSA and by both the Department of Defense and the Office of the DNI by agency inspectors general, general counsels, compliance officers and privacy officers (including my office and the NSA's new Civil Liberties and Privacy Office). The Department of Justice also provides oversight, as do the Privacy and Civil Liberties Oversight Board and the president's Intelligence Oversight Board. In addition, Congress has the power to oversee, authorize and fund these activities.

Many of these protections apply expressly to information about U.S. persons. This is to be expected, in light of our legal framework and the need to ensure that foreign intelligence agencies protect national security without interfering with our democratic processes and our values. But intelligence agencies pursue their missions in a manner that provides important safeguards for all personal information. Indeed, the NSA's extensive internal compliance system enforces key protections regardless of nationality, as shown by the letter recently issued by the NSA inspector general. That letter reported on the small number of cases over the past decade in which government employees had intentionally violated prohibitions on searching signals intelligence information; in several cases, employees were held accountable for improperly searching for information about foreign nationals.

Tye stated that none of President Obama's recent reforms affect 12333 collection. In fact, the president recently issued Presidential Policy Directive 28 (PPD-28), which covers EO 12333 signals intelligence (SIGINT) collection. It requires that SIGINT activities be as tailored as feasible, limits the use of SIGINT information collected in bulk and directs intelligence agencies to safeguard personal information collected through SIGINT, regardless of nationality.

EO 12333 plays an important role in America's intelligence oversight framework, so that, in the words of the order, agencies execute their missions "in a vigorous, innovative, and responsible

manner that is consistent with the Constitution and applicable law and respectful of the principles upon which the United States was founded."

Tye called for a debate about EO 12333. We welcome that debate. But let's conduct it based on facts.

Alexander Joel is the civil liberties protection officer for the Office of the Director of National Intelligence and reports directly to Director of National Intelligence James R. Clapper. As the leader of the ODNI's Civil Liberties and Privacy Office, Joel's oversight responsibilities include ensuring that privacy and civil liberties protections are incorporated in Intelligence Community policies and procedures, overseeing compliance by the ODNI with privacy and civil liberties laws, reviewing complaints of possible abuses of privacy and civil liberties in programs and operations administered by the ODNI, and ensuring that the use of technology sustains, and does not erode, privacy.